



## Withdrawn paper: fast multiplication of integer matrices

Joris van Der Hoeven

### ► To cite this version:

Joris van Der Hoeven. Withdrawn paper: fast multiplication of integer matrices. 2012. hal-00742099v2

**HAL Id: hal-00742099**

**<https://hal.science/hal-00742099v2>**

Preprint submitted on 2 Nov 2012

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# FAST MULTIPLICATION OF INTEGER MATRICES

## Withdrawn paper

*Joris van der Hoeven*

Laboratoire d'informatique  
UMR 7161 CNRS  
École polytechnique  
91128 Palaiseau Cedex  
France

*Email:* [vdhoeven@lix.polytechnique.fr](mailto:vdhoeven@lix.polytechnique.fr)

*Web:* <http://www.lix.polytechnique.fr/~vdhoeven>

*November 2, 2012*

---

In this paper we will show that dense  $n \times n$  matrices with integer coefficients of bit sizes  $\leq b$  can be multiplied in quasi-optimal time. This shows that the exponent  $\omega_{\mathbb{Z}}$  for matrix multiplication over  $\mathbb{Z}$  is equal to two. Moreover, there is hope that the exponent can be observed in practice for a sufficiently good implementation.

KEYWORDS: matrix multiplication, FFT, skew polynomials

A.M.S. SUBJECT CLASSIFICATION: 15-04, 68Q25, 68W30

---

**Erratum.** Eric SCHOOST discovered a bug in this paper: by construction, formula (7) does not hold, since the matrix  $V_{a,n}$  is not invertible whenever  $l \geq 2$ . Unfortunately, we do not see how to repair this bug: not only  $V_{a,n}$  is not invertible, but the rank of  $V_{a,n}$  is actually very small (and equal to  $\max\{q_1, \dots, q_l\}$ ). This makes the proof collapse.

We have also tried a few other things, such as fixing  $a = 2$  and trying to take many  $q_i$  for which  $a$  is a primitive root of unity of a small order. This also does not work, since the product of two operators in  $\mathbb{Z}[X, Q]_2$  makes the coefficient sizes increase by  $n^2$  (and not merely  $n$ ) bits. Going until “small order  $n$ ”, we must have  $q_1 \cdots q_l \mid \text{lcm}(2^1 - 1, 2^2 - 1, \dots, 2^n - 1)$ . This lcm is of the same order as  $2^{n^2}$ , but strictly smaller than  $2^{n^2}$ .

## 1. INTRODUCTION

### 1.1. Main results

Let  $\mathbb{A}$  be an effective ring, which means that there exist algorithms for performing all ring operations. It is classical that there exist quasi-optimal algorithms for many kinds of computations with polynomials over  $\mathbb{A}$ . For instance, two polynomials of degrees  $< n$  can be multiplied using  $M_{\mathbb{A}}(n) = \mathcal{O}_{\mathbb{A}}(n \log n \log \log n)$  operations in  $\mathbb{A}$  [5, 17, 6, 13]. If  $\mathbb{A}$  admits primitive  $2^p$ -th roots of unity for any  $p$ , then we even have  $M_{\mathbb{A}}(n) = \mathcal{O}_{\mathbb{A}}(n \log n)$ . From the complexity point of view, multiplication is the central operation: good bounds for the complexities of division, g.c.d., multipoint evaluation, etc. are known in terms of the complexity of multiplication.

































